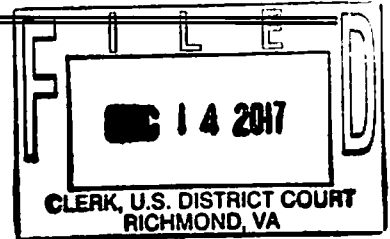


## UNITED STATES DISTRICT COURT

for the  
Eastern District of Virginia

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

12917 Crowne Ridge Loop, Apartment 302  
Midlothian, VA 23112

Case No. 3:17SW266

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, fully incorporated by reference herein;

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, fully incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. § 841	Distribution of Controlled Substances
21 U.S.C. § 846	Conspiracy to Distribute Controlled Substances
18 U.S.C. § 1028(a)(5)	Fraud and Related Activity in Connection with Authentication Features

The application is based on these facts:

See attached Affidavit, fully incorporated by reference herein.

- ☐ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

John McCormack, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 12/14/2017

City and state: Richmond, Virginia

Roderick C. Young  
United States Magistrate Judge

Judge's signature

Roderick C. Young, United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Richmond Division

IN THE MATTER OF THE SEARCH OF:  
The premises known as  
12917 Crowne Ridge Loop, Apartment 302  
Midlothian, VA 23112

Case No. 3:17SW266

**FILED UNDER SEAL**

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER  
RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, John McCormack, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 12917 Crowne Ridge Loop, Apartment 302, Midlothian, Virginia 23112, hereinafter "SUBJECT PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a special agent of the Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), currently assigned to the Office of the Assistant Special Agent in Charge Norfolk, in the Richmond, Virginia Office. I have been employed as an HSI special agent since November 2011. Prior to that, I served as a special agent with the Defense Criminal Investigative Service ("DCIS") since 2004. As part of my daily duties as an HSI agent, I investigate criminal violations relating to the illegal possession with the intent to distribute controlled substances and conspiracy to distribute controlled substances, in violation of 21 U.S.C. § 841 and 21 U.S.C. § 846.

3. In the course of my employment as a sworn law enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of controlled substances, drug paraphernalia, computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including various sections of Title 21, United States Code, U.S.C. § 841 involving possession with the intent to distribute controlled substances, and Title 18, U.S.C § 1028 involving fraud in connection with identification documents.

4. The statements in this affidavit are based in part on my investigation of this matter and on information provided by other law enforcement agents. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence, contraband, and instrumentalities of violations of 21 U.S.C. § 841, 21 U.S.C. § 846 and 18 U.S.C § 1028 are presently located at the SUBJECT PREMISES.

5. The purpose of the application which this affidavit supports is to obtain court authorization to seize evidence, more particularly described in Attachment B, of violations of 21 U.S.C. § 841 which make it a crime to possess controlled substances with the intent to distribute, 21 U.S.C. § 846, which make it a crime to conspire to distribute a controlled substance, and 18 U.S.C § 1028(a)(5), which make it a crime to knowingly and unlawfully produce or distribute authentication features associated with access devices. I am requesting authority to search the entire premises, including the residential dwelling and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as contraband, instrumentalities, and evidence of a crime.

6. In summary, the following affidavit sets forth facts that establish that there is probable cause to believe that there is a subject using the residence at 12917 Crowne Ridge Loop, Apartment 302, Midlothian, Virginia 23112, to manufacture and to distribute controlled substances and using a computer or electronic device that is presently located at the SUBJECT PREMISES.

#### **RELEVANT STATUTORY PROVISIONS**

7. **Distribution of Controlled Substances:** 21 U.S.C. § 841 provides it shall be unlawful for any person knowingly or intentionally to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute, or dispense, a controlled substance.

8. **Conspiracy to Distribute Controlled Substances:** 21 U.S.C. § 846 provides that any person who attempts or conspires to commit a drug distribution offense shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

9. **Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information:** 18 U.S.C. § 1028(a)(5) provides that it shall be unlawful for any person to produce, transfer or possess a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature which will be so used.

#### **DEFINITIONS**

10. The **Internet** is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices

on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

11. **Internet Protocol address (or simply “IP address”)** is a unique numeric address used by computers on the Internet. A typical IP address looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Newer IP addresses use a IPv6 format, represented as eight groups of four hexadecimal digits with the groups being separated by colons, for example 2001:0db8:0000:0042:0000:8a2e:0370:7334. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

12. **Storage medium** is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

13. **Log Files** are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

14. **Internet Service Providers or ISPs** are commercial organizations, which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone-based dial-up, broadband-based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

15. **Tor** is free software for enabling anonymous communication. The name Tor is an acronym for the original software project named "The Onion Router." Tor directs internet traffic through a free, worldwide, overlay network consisting of thousands relays, also called "nodes," that conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace internet activity back to the actual user: this includes visits to Web sites, online posts, instant messages, and other communication forms. When internet traffic enters the Tor network, Tor encrypts the data, including the next node destination IP address, multiple times and sends it through a virtual circuit comprising successive, random-selection Tor relays. Each relay decrypts a layer of encryption to reveal the next relay in the circuit to pass the remaining encrypted data on to it. The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing or

knowing the source IP address.

16. **Tor Hidden Services:** The Tor network can also provide anonymity to websites and other servers. Servers configured to receive inbound connections only through Tor are called hidden services. Rather than revealing a server's true IP address (and thus its network location), a hidden service is accessed through something called an onion address<sup>1</sup>, usually via the Tor Browser. The Tor network understands these addresses and routes data to and from hidden services, even those hosted behind firewalls or network address translators (NAT), while preserving the anonymity of both parties. Tor is necessary to access hidden services, and because hidden services do not use exit nodes, which are relays used when internet traffic enters or leaves the Tor network, connection to a hidden service is encrypted end-to-end.

17. **Darknet and Dark Web Markets.** The term "darknet" describes servers and activity on the internet that are only accessible through special software like Tor and which typically cannot be indexed and searched by search engines like Google, Yahoo and Bing. A synonymous term for "darknet" is "dark web." A "darknet market" is a commercial website on the web that operates via darknets such as Tor or another anonymizing network. Darknet markets function primarily as black markets, selling or brokering transactions involving drugs, child pornography, hacking tools and malware, firearms, counterfeit currency, stolen credit card information, forged documents, unlicensed pharmaceuticals, steroids, and other illicit goods and services.

18. **Smartphone** is a portable personal computer with a mobile operating system

---

<sup>1</sup> Tor uses a special top-level domain suffix ".onion" in place of conventional domain suffixes like ".com," ".net," or ".gov." The .onion suffix designates an anonymous hidden service reachable via the Tor network.

having features useful for mobile or handheld use. Smartphones, which are typically pocket-sized (as opposed to tablets, which are larger in measurement), have become commonplace in modern society in developed nations. While the functionality of smartphones may vary somewhat from model to model, they typically possess most if not all of the following features and capabilities: 1) place and receive voice and video calls; 2) create, send and receive text messages; 3) voice-activated digital assistants (such as Siri, Google Assistant, Alexa, Cortana, or Bixby) designed to enhance the user experience; 4) event calendars; 5) contact lists; 6) media players; 7) video games; 8) GPS navigation; 9) digital camera and digital video camera; and 10) third-part software components commonly referred to as “apps.” Smartphones can access the Internet through cellular as well as Wi-Fi (“wireless fidelity”) networks. They typically have a color display with a graphical user interface that covers most of the front surface of the phone and which usually functions as a touchscreen and sometimes additionally as a touch-enabled keyboard.

19. **SIM card** stands for a “subscriber identity module” or “subscriber identification module,” which is the name for an integrated circuit used in mobile phones that is designed to securely store the phone’s international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contact information on many SIM cards.

20. The terms “**records**,” “**documents**,” and “**materials**,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures,



photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Smartphones, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

21. **“Vendors”** are the dark web’s sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of “vendor accounts.” Customers, meanwhile, operate “customer accounts.” It is possible for the same person to operate one or more customer accounts and one or more vendor accounts at the same time.

22. **“Bitcoin”** (or “BTC”) is an online digital currency, also called a cryptocurrency, that allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems. Bitcoins are a decentralized, peer-to-peer form of electronic currency having no association with banks or governments. Unlike “fiat” currencies, which derive value and consumer faith from the fact that they are backed by the central government that issued them, bitcoin and other cryptocurrencies derive value and consumer faith, in part, because all transactions are publically viewable in a secure, open distributed ledger called a “blockchain.” Users store their bitcoins in digital “wallets,” which are identified by unique electronic “addresses.” Although they are legal and have known legitimate uses, bitcoins are also known to be used by cybercriminals for money-laundering purposes, and are believed to be the most oft-used means of payment for illegal goods and services on “dark web” websites operating on the Tor network. By maintaining multiple bitcoin wallets, those who use bitcoins for illicit purposes

can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplace. As of December 12, 2017, one bitcoin is worth approximately \$17,700, though bitcoins' value is much more volatile than that of fiat currencies.

23. **"Bitcoin exchanges"** are companies that allow users to trade bitcoins for other currencies, including U.S. dollars. Although criminals—including dark web vendors of illicit goods and services—may use Bitcoin exchanges to launder the proceeds of their crimes, many legitimate bitcoin exchanges have implemented "Know Your Customer" (or "KYC") protocols and other verification procedures similar to those employed by traditional financial institutions. For example, "Bitstamp," founded in Slovenia and now based in Luxembourg, requires users who want to open or maintain accounts on the exchange to provide information and supporting documentation about their identities, finances, and sources of bitcoins, among other things. Because there is still market demand for anonymous bitcoin-to-dollar exchanges, however, vendors on dark web marketplaces can offer that service, allowing customers to exchange digital and fiat currencies with none of the anti-money laundering protections that exist in the traditional banking system. These vendor-exchanges are often able to charge a higher fee for the service because customers who obtain their bitcoins through criminal activity—such as drug dealing on the dark web—are willing to pay for greater financial secrecy.

**COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

24. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is digital data stored on a computer's hard drive or other storage media, or on a smartphone's internal memory or SIM card. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

25. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

Depending on a variety of factors, a particular computer could easily not overwrite deleted files with new data for many months, and in certain cases conceivably ever.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the

storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about

how computers were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to possess, receive, distribute and/or produce child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or

received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

27. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways,

featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.



29. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

**SPECIFICITY OF SEARCH WARRANT RETURN AND NOTICE REGARDING  
INITIATION OF FORENSIC EXAMINATION**

30. Consistent with the Court's current policy, the search warrant return will list the model(s) and serial number(s) of any and all computers seized at the SUBJECT PREMISES, and include a general description of any and all associated peripheral equipment that has been seized. Additionally, the search warrant return will include the total numbers of each type of digital media that has been seized (*e.g.*, "ten (10) 3.5" diskettes; twenty (20) CDs; twenty (20) DVDs; three (3) USB drives; one (1) 256 MB flash memory card," *etc.*)

31. Moreover, the Government will file a written pleading in this case within one hundred twenty (120) days after the execution of the search warrant notifying the court that the imaging process of digital evidence seized from the target location is complete, and the forensic analysis of computers and media has begun. Such notice will include confirmation that written notice has been provided to the defendant or his counsel informing the defendant that the forensic examination of evidence seized from him has actually begun. Such notice to the defendant and the Court is not intended to mean, and should not be construed to mean, that the forensic analysis is complete, or that a written report detailing the results of the examination to date will be filed with the Court or provided to the defendant or his counsel. This notice does not create, and is not meant to create, additional discovery rights for the defendant. Rather, the sole

purpose of this notice is to notify the defendant that, beyond the simple seizure of his property, a forensic search of that property has actually begun.

**PROBABLE CAUSE**

32. Beginning around July 2017, I began investigating information received from a special agent assigned to the HSI New York field office (“HSI-NY”), who is working on a joint HSI and United States Postal Inspection Service (“USPIS”) certified undercover (“CUC”) operation. HSI-NY and USPIS have been investigating widespread importation and online distribution of pharmaceuticals and other controlled substances (including sales on dark web marketplaces such as AlphaBay, Dream and Hansa as well as the laundering of illicit proceeds of these drug crimes (including digital-currency proceeds such as bitcoin), occurring across the country, including the Eastern District of Virginia.

33. HSI-NY special agents operating an undercover Dark Net Market (DNM) vendor account on Hansa, AlphaBay, Dream, *et al.*, receive incoming BTC purchase requests from various individuals operating on the Dark Net. These individuals place an order for U.S. currency in exchange for bitcoin, for a negotiated fee based on a percentage of the total funds. Once the purchaser makes the request on the DNM, HSI-NY special agents assign the transaction an internal identifying transaction number. The DNM transaction initiates the transfer of the specified amount of bitcoin into an escrow account or a 2-3 multi-sig escrow wallet<sup>2</sup>, depending on the marketplace. The purchaser also provides a name and address to

---

<sup>2</sup> Standard transactions on the bitcoin network are single-signature transactions because transfers require only one signature, *i.e.*, that of the owner of the private key associated with the bitcoin address. However, bitcoin offers the option to create a wallet that requires more than one person’s authority to authorize a transaction. The term for such wallets is “multi-sig” (also referred to as “multisignature” or “multisig”). The idea is that bitcoins become “encumbered” by

which the U.S. currency is to be mailed.

34. HSI special agents then withdraw the specified amount of U.S. currency from a CUC bank account and transport the currency to the HSI-NY office for processing. Once recounted and packaged for shipping to the specified address, the currency is then transported to one of several local post offices or one of several FedEx locations to be sent. The FedEx tracking number is monitored by HSI special agents to ensure delivery of the package.

35. Once the order is completed, the remaining bitcoin, less any marketplace fees, is transferred from the escrow or multi-sig wallet to a "release" wallet controlled by HSI-NY special agents. As noted above, all bitcoin transactions are recorded in an open, distributed ledger called the blockchain, which anyone can publically view. To ensure proper blockchain obfuscation, HSI-NY special agents transfer the balance of bitcoin through multiple undercover HSI-controlled accounts on LocalBitcoins.com, which is a bitcoin trading website. HSI-NY special agents then transfer the remaining bitcoin, less any fees, to an operation executive CUC Coinbase account wallet maintained and controlled by an HSI-NY special agent.

36. The CUC bank account is then reviewed by HSI-NY special agents to ensure the final deposit from the CUC Coinbase account has been made. The final deposit amount is minus any market or processing fees associated with the BTC transaction, and any positive or negative deposit amount, subtracting the transaction request aggregate, reflects realized proceeds or loss for accounting purposes.

37. On July 31, 2017, I received information from HSI-NY that they were shipping, via United States Postal Service (USPS), a package containing \$1,000 in U.S. currency to Mark

---

providing addresses of multiple parties, thus requiring cooperation of those parties in order to do anything with them.

FAULKNER, 12917 Crowne Ridge Loop, Apt 302, Midlothian, VA 23112. The package was for a Bitcoin-to-U.S. Currency transaction for an order received from the dark web market Dream using the moniker "titbodge." HSI-NY provided me with the USPS tracking number, picture of the package and the approximate date of delivery.

38. On August 2, 2017, Customs and Border Protection (CBP) Officer Kirsten Clemens and I initiated a surveillance of the mailboxes located at the Crowne at Swift Creek apartment complex in Chesterfield County, where 12917 Crowne Ridge Loop, Apt. 302 is located. While on surveillance, I witnessed a USPS vehicle drive up to the apartment complex mailboxes and a USPS employee deliver a package matching the description of the package send by HSI-NY to the mailbox assigned to FAULKNER at 12917 Crowne Ridge Loop, Apt 302.

39. On August 7, 2017, I received further information from HSI-NY that they were shipping a second package, also via USPS, containing \$2,000 in U.S. currency to FAULKNER at the 12917 Crowne Ridge Loop, Apt 302, address. This package also for a Bitcoin-to-U.S. Currency transaction for an order received from dark web market Dream, using the moniker "titbodge." HSI-NY again provided me with the USPS tracking number, picture of the package and the approximate date of delivery.

40. On August 9, 2017, CBP Officer Clemens and I conducted a second surveillance of the mailboxes located at the Crowne at Swift Creek apartment complex. While on surveillance, I witnessed a USPS vehicle drive up to the apartment complex mailboxes and a USPS employee deliver the second package matching the description of the package send by HSI-NY to the mailbox assigned to FAULKNER at 12917 Crowne Ridge Loop, Apt. 302.

41. During this time, I received information from HSI-NY concerning two other Bitcoin-to-U.S. Currency transactions that occurred on June 14, 2017, and July 15, 2017. The June 14, 2017 Bitcoin transaction was from dark web market ALPHA BAY, using the moniker "Chang1927," and was for \$500.00 in U.S. Currency. The July 15, 2017 Bitcoin-to-U.S. Currency transaction was from dark web market Dream, using the moniker "Chang1927," for \$1,000 in U.S. Currency.

42. On August 7, 2017, I received information from HSI-NY that they had discovered the dark web market Dream vendor account for "Chang1927." HSI-NY stated that they planned to conduct an undercover purchase from "Chang1927" of prescription fentanyl.

43. On September 13, 2017, I received information from HSI-NY that they had made an undercover purchase of fentanyl from dark web market Dream vendor "Chang1927." On September 7, 2017 HSI-NY seized two (2) packages, one (1) containing an eye dropper bottle and the other containing two (2) nasal spray bottles, each suspected to contain liquid fentanyl. Both packages had the return mailing address of 12917 Crowne Ridge Loop, Midlothian, VA 23112. HSI-NY submitted the bottles of suspected fentanyl to the DEA Laboratory for analysis and the packaging material to the HSI Forensics Laboratory for latent fingerprint analysis.

44. On October 11, 2017, the Chesterfield County Police Department (CPD) responded to a 911 call for an unresponsive male locked in the bathroom at the residence of FAULKNER and THY HOANG, 12917 Crowne Ridge Loop, Apartment 302, Chesterfield, Virginia. Upon entering the residence, HOANG, who is FAULKNER'S wife, reported to the CPD officer that FAULKNER had entered the bathroom for a while and did not respond when she knocked on the door. The CPD officer observed EMS personnel who were on scene

assisting an unresponsive FAULKNER from the bathroom to the bed. FAULKNER was unable to provide any explanation for his condition. The CPD officer observed that FAULKNER had a white residue on his nose, and further saw a plastic bag containing a white substance in the bathroom.

45. The CPD officer also observed two white, unmarked bottles of nasal spray in the bathroom. At the time of the incident, the officer did not appreciate the significance of the unmarked bottles of nasal spray, and therefore he neither seized nor photographed the bottles. Federal investigators inquiring into FAULKNER's online distribution of fentanyl have since interviewed the CPD officer who responded to FAULKER's home following the 911 call. The officer identified photos of nasal spray bottles containing fentanyl sold on multiple dark web markets as being very similar in appearance, if not identical, to the white nasal spray bottles he saw in FAULKNER's bathroom that day.

46. Record checks conducted on THY HOANG indicated that she was a registered pharmacy technician in Texas, registration number 164042, from August 28, 2008, to May 31, 2010.

47. On November 20, 2017, I received information from HSI-NY concerning the fingerprint and lab analysis of the suspected fentanyl shipments. The HSI Forensics Laboratory report stated that four (4) latent fingerprints were identified on one of the packages, with three (3) of those prints belonging to FAULKNER. The DEA Laboratory Report states that the three (3) bottles seized on September 7, 2017, contained an approximate total of 53.3 grams of cyclopropylfentanyl (fentanyl).

48. On December 12, 2017, FBI Special Agent Jeremy D'Errico conducted open-source research on the Darknet market Dream user "Chang1927." The Darknet market Dream

profile for “Chang1927” listed December 11, 2017, as the “last active” date.

49. On December 13, 2017, SA D’Errico conducted open-source research on the user “Chang1927” on a separate darknet market named Zion. The darknet market Zion profile for “Chang1927” listed December 13, 2017, as the “last login” date. The user “Chang1927” listed four products for sale:

- a. Adderall XR 30mg Extended Release Pharmacy Grade - \$27
- b. Fentanyl HCL 98% Pure Spray 30mg Express Shipping Available - \$150
- c. Fentanyl HCL 98% Pure Spray 100mg - \$400
- d. 2017 FRAUD PACK 75,000 ITEMS/32GB ANTI-DETECT 7.0/98 CC/CCV - \$20

50. The advertisements for fentanyl are similar in the form and amounts of fentanyl previously offered by user “Chang1927” on the Darknet market Dream.

51. The advertisement for the 2017 FRAUD PACK is further described, in part, as:

[A] massive package of high quality material for faking, making, and counterfeiting almost anything. This is a list of just some of its contents: Multiple ID, passport, and License scans from each US state and many other countries, almost 300 International Passport scans from 46 countries including USA, SS Cards, licenses, US Military, University and College ID scans, Birth Certificates, Professional Certifications, Diplomas, Transcripts, Car Insurance, Utility Bills, Vehicle Registrations, Bar-code Software, Receipts, CC Verifier, Credit Card Printing, UV Scans, Tons of Credit Card Templates Front and Back (Visa, AMex, Discover, Master Card, CitiBlack, Silver, Gold, Platinum, Travelers Checks, All USD and EUR Counterfeit Money Templates, Counterfeit Paper, Pin Cracking, Hundreds of Programs For Faking, and thousands more items.

In addition, I understand “CC/CVV” to mean credit card/card verification value, which is a three to four digit code printed on the reverse side of a credit card used to validate that a cardholder has physical possession of the credit card. In addition to credit and debit account numbers themselves, CC/CCV codes are often bought and sold on darknet markets for individuals to

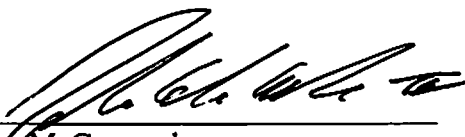
engage in access device fraud.

### **CONCLUSION**

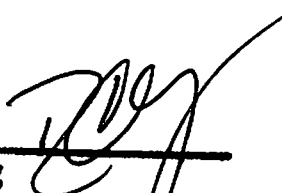
52. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that (1) an individual or individuals at the SUBJECT PREMISES used a computer or electronic device connected to the Internet from the SUBJECT PREMISES to violate Title 21, United States Code §§ 841 and 846, Title 18 United States Code § 1028, and (2) the fruits, evidence, contraband and instrumentalities of these offenses, described in Attachment B, are presently located at the SUBJECT PREMISES. Permission is expressly sought to seize any controlled substances, drug paraphernalia, shipping records, shipping materials, computer hardware, computer software, and computer related documentation located at the SUBJECT PREMISES and subsequently conduct an on-site and off-site forensic examination, as necessary, using whatever data analysis techniques are needed to seize the contraband, evidence, and instrumentalities listed in Attachment B.



53. I respectfully request, therefore, that the Court issue the attached warrant authorizing the search and seizure of the items listed in Attachment B.

  
\_\_\_\_\_  
John McCormack  
Special Agent  
Homeland Security Investigations

SUBSCRIBED and SWORN  
before me on December 14, 2017

  
\_\_\_\_\_  
/s/  
Roderick C. Young  
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Richmond Division

IN THE MATTER OF THE SEARCH OF:

The premises known as  
12917 Crowne Ridge Loop, Apartment 302  
Midlothian, VA 23112

Case No. 3:17SW266

**FILED UNDER SEAL**

**ATTACHMENT A**

**DESCRIPTION OF PREMISES TO BE SEARCHED**

The premises to be searched is known as 12917 Crowne Ridge Loop, Apartment 302, Midlothian, VA 23112. The premises is described as a three-story apartment building, with 12 individual units, four on each floor. The premises has a brick and grey siding exterior. The front of the premises has the number 12917 in large numbers above the open-air entrance/staircases. On the left of building 12917 is building 12913 and on the right is building 12919. The apartment located on the 3rd floor (top floor), on the back left side of the building, when looking at the front of the building. The front entry door is recessed and dark green in color. The numbers "302" are attached to the upper half of the door above the doorknocker. A picture of 12917 Crowne Ridge Loop, Apartment 302 is attached.

**Attachment A**

**DESCRIPTION OF PREMISES TO BE SEARCHED**



**Front View of 12917 Crowne Ridge Loop, Midlothian, VA**



**Rear View of 12917 Crowne Ridge Loop, Midlothian, VA**

**Attachment A**

**DESCRIPTION OF PREMISES TO BE SEARCHED**



**View of Front Entrance, 12917 Crowne Ridge Loop, Apt 302**



**View of Front Door of 12917 Crowne Ridge Loop, Apt 302**

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Richmond Division

IN THE MATTER OF THE SEARCH OF:

The premises known as  
12917 Crowne Ridge Loop, Apartment 302  
Midlothian, VA 23112

Case No. 3:17SW266

**FILED UNDER SEAL**

**ATTACHMENT B**

*Property to be seized*

1. All records relating to violations of 21 U.S.C. §§ 841 and 846 relating to the illegal possession with the intent to distribute controlled substances and conspiracy to distribute controlled substances, and 18 U.S.C § 1028 relating to fraud and related activity in connection with identification documents, authentication features, and information including:

- a. books, records, receipts, notes, ledgers, and other papers relating to the transporting, ordering, purchasing, and distributing of controlled substances;
- b. books, records, invoices, receipts, records of real estate transactions (whether rented or owned property), bank statements and related records, passbooks, money drafts, letters of credit, money orders, bank drafts, and cashier's checks, bank checks, safe deposit box keys, money wrappers, and other items evidencing the obtaining, secreting, transferring, and/or concealment of assets and the obtaining, secreting, transferring, concealing, and/or expending of money;

- c. photographs, including still photographs, negatives, video tapes, films, undeveloped film and the contents therein, slides, in particular photographs of co-conspirators, assets, and/or controlled substances;
  - d. address and/or telephone books, rolodex indices and any papers reflecting names, addresses, telephone numbers, pager numbers, fax machines, and/or telex numbers of co-conspirators, sources of supply, customers, financial institutions, and other individuals or businesses with whom a financial relationship exists;
  - e. indicia of occupancy, residency, rental, and/or ownership of the premises to be searched, including, but limited to, utility and telephone bills, cancelled envelopes, rental, purchase, or lease agreements, and keys;
  - f. records and information relating to the dark web market vendor accounts “Chang1927” and “titbodge”;
  - g. credit card numbers, templates, holograms, blank magnetic cards, magnetic card encoders, authentication features, document-making implements, or any other information/device used to facilitate the collection, manufacturing, or distribution of identification documents, personal identification card, or means of identification.
- 2. Any and all suspected controlled substances;
  - 3. Scales, containers, mixers, cutting tools, packaging materials, beaters, burners, and any other drug paraphernalia used in manufacturing, diluting, packaging, and distributing

controlled substances;

4. Computers or storage media used as a means to commit the violations described above.

5. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

- f. evidence of the times the COMPUTER was used;
  - g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
  - h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
  - i. records of or information about Internet Protocol addresses used by the COMPUTER;
  - j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
  - k. contextual information necessary to understand the evidence described in this attachment;
  - l. Presence of Bitcoin or other virtual currency.
6. Routers, modems, and network equipment used to connect computers to the Internet.
7. Cellular telephones, portable cellular telephones, electronics pagers, and any stored electronic communications contained therein;
8. United States currency, precious metals, jewelry, and financial instruments, including stocks and bonds;



9. During the course of the search, law enforcement officials may photograph the searched SUBJECT PREMISES to record the condition thereof and/or the location of items therein.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.